New gTLD Program Safeguards Against DNS Abuse

ICANN Operations and Policy Research | March 2016

# ICANN CCT Review

## Consumer **Trust** - Sub-team

Note that this report is meant as an ***aid*** to the CCT-RT.

# Consumer TRUST

- Will new gTLDs **erode** trust?

- Will Safeguards avoid abuse? What other Remedies do we have?

- Definition DNS Abuse?

- Abuse is an action that: a) causes actual and substantial harm, or is a material predicate of harm, and b) Is illegal or illegitimate, or is otherwise contrary to the intention and design of a stated legitimate purpose, if such purpose is disclosed. *(2010, GNSO's Registration Abuse Policies Working Group (RAPWG) Report)*

A 2015 ICANN-sponsored global survey of 6,144 consumers reported

- 74% were aware of phishing
- 79% were aware of spamming
- 40% were aware of *cybersquatting*
- 67% were aware of stolen credentials
- 76% were aware of malware

Researchers from the University of California, San Diego found that **new TLD domains are more than twice as likely as legacy TLDs to appear on a domain blacklist**—a list of domains of known spammers— within their first month of registration.

Stakeholders: Anti-Phishing Working Group (APWG), the Registry Internet Safety Group (RISG), the Security and Stability Advisory Committee (SSAC), Computer Emergency Response Teams (CERTs) and members from the banking, financial, and Internet security communities

# Specification 11 RA

New gTLD Registry Agreement mandates that registry operators commit to certain public interest commitments (PICs) as part of their contractual obligations with ICANN. Sub-sections 3a and 3b:

- …..a provision prohibiting Registered Name Holders from **distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law,** and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.
- …..periodically conduct a technical analysis to assess whether domains in the TLD are being used to **perpetrate security threats, such as pharming, phishing, malware, and botnets**. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks.

The activities described within Specification 11 may provide an additional definitional framework for the CCT-RT as they refine the scope of their review.

# Any other Safeguards down at the retail and end user level????

- QUESTION: HOW DO WE ENSURE THAT BAD ACTORS DO NOT RUN REGISTRIES?
- SAFEGUARD: **VET REGISTRY OPERATORS**
- QUESTION: HOW DO WE ENSURE INTEGRITY AND UTILITY OF REGISTRY INFORMATION?
- SAFEGUARD: **REQUIRE DEMONSTRATED PLAN FOR DNSSEC DEPLOYMENT**
- SAFEGUARD: **PROHIBITION OF WILDCARDING**
- SAFEGUARD: **REMOVAL OF ORPHAN GLUE RECORDS**
- QUESTION: HOW DO WE ENSURE MORE FOCUSED EFFORTS ON COMBATING IDENTIFIED ABUSE?
- SAFEGUARD: **REQUIREMENT FOR THICK WHOIS RECORDS**
- SAFEGUARD: **CENTRALIZATION OF ZONE-FILE ACCESS**
- SAFEGUARD: **DOCUMENTED REGISTRY LEVEL ABUSE CONTACTS AND PROCEDURES**
- SAFEGUARD: **PARTICIPATION IN AN EXPEDITED REGISTRY SECURITY REQUEST PROCESS (ERSR)**
- QUESTION: HOW DO WE PROVIDE AN ENHANCED CONTROL FRAMEWORK FOR TLDS WITH INTRINSIC POTENTIAL FOR MALICIOUS CONDUCT?
- SAFEGUARD: **CREATE A DRAFT FRAMEWORK FOR A HIGH SECURITY ZONE VERIFICATION PROGRAM**

# ICANN **Draft** Report
# New gTLD Program **Safeguards** to Mitigate DNS **Abuse**

- Written by ICANN staff March 2016, explores methods for **measuring** the effectiveness of 9 safeguards implemented as part of the New gTLD Program

- It defines the activities that constitute **DNS abuse** (at **registration**, as well as **use** after created) and assesses **indicators** of the rate of abuse.

- Also explores user feedback with these safeguards and presents additional proposals for researching how these safeguards might be affecting abuse **rates.** METRICS: 66 new gTLD metrics (III. domain abuse), Health Index, etc.

# Effectiveness of the SPEC 11 safeguards to mitigate DNS abuse

*“It remains to the CCT-RT to decide the scope and method of their inquiry into DNS abuse mitigation efforts”*

## Causal Models and Hypotheses

The models below derive from a simple central hypothesis that—theoretically at least—the introduction of safeguards to prevent DNS abuse in new gTLDs should result in a “cleaner” (i.e. fewer malicious activities) DNS space compared to the “legacy” TLD era when such safeguards did not exist.

# What are we missing?

~~THRUST!!!~~

DATA
(time series)